IN THE CLAIMS:

1. (Currently amended) A method in a network device for caching Hyper Text Transfer Protocol (HTTP) data transported in an Internet Protocol (IP) Datagram sent on a socks connection established over a Transmission Control Protocol (TCP) connection between a source port on a source device and a destination port on a destination device, said method comprising the steps of:

identifying elements of an incoming IP Datagram, comprising:

the source device[[,]];

the destination device[[,]];

the port on the source device[[,]]; and

the port on the destination device[[,]];

~~of an incoming IP Datagram.~~

determining whether the incoming IP Datagram ~~is originated by~~ originates from a socks client or [[by]] from a socks server[[:]];

in response to [[If]] the incoming IP Datagram ~~is originated by~~ originating from a socks client:

terminating the TCP connection and the socks connection;

identifying the socks connection in a table;

identifying the application level protocol associated with said socks connection referring to said table, said table comprising for each socks connection an application level protocol; and

determining whether said application level protocol is HTTP or not[[:]];

in response to [[If]] said application level protocol [[is]] being HTTP:

determining whether HTTP data requested by the incoming IP Datagram [[is]] resides in a local cache within the network device[[:]]; and

in response to the [[If]] HTTP data requested by the incoming IP Datagram [[is]] residing in a local cache:

building an outgoing IP Datagram comprising requested HTTP data retrieved from the local cache; and

sending said outgoing IP Datagram to the socks client originator of the incoming IP Datagram.

2. (Currently amended) The method according to ~~the preceding~~ claim 1, wherein: in response to the [[If]] HTTP data requested by the IP Datagram [[are]] not residing in the local cache within the network device:

identifying the outbound socks connection associated with the socks connection referring to the table, said table comprising for each socks connection an outbound socks connection[[.]];

building an outgoing IP Datagram with information comprised in the incoming IP Datagram; and

sending said outgoing IP Datagram on the outbound socks connection.

3. (Currently amended) The method according to ~~any one of the preceding claim 2~~ claim 1, wherein said step of identifying the socks connection in a table, comprises the further steps of:

determining whether the IP Datagram comprises a message for establishing a new socks connection, in particular a socks CONNECT message, or not; and

if the incoming IP Datagram comprises a message for establishing a new socks connection, in particular a socks CONNECT message:

defining an inbound socks connection between the socks client source of the incoming IP Datagram and the network device; and

updating the table with:

an identification of the socks connection;

an identification of the associated inbound socks connection; and

the application level protocol associated with the socks connection.

4. (Currently amended) The method according to claim 2, wherein said step of identifying the outbound socks connection associated with the socks connection referring to the table comprises the further steps of:

defining an outbound socks connection between the network device and the destination device of the incoming IP Datagram; and

associating in the table said outbound socks connection [[(604)]] with the socks connection of the incoming IP Datagram.

5. (Currently amended) The method according to claim 2, wherein:

in response to [[]f]] the incoming IP Datagram ~~is originated by~~ not originating from a socks server:

terminating the TCP connection and the socks connection;

identifying the socks connection in the table;

identifying the application level protocol associated with said socks connection referring to said table; and

determining whether said application level protocol is HTTP[[:]]; and

in response to [[]f]] said application level protocol [[is]] being HTTP:

caching HTTP data comprised in incoming IP Datagram in the local cache of the network device;

identifying the inbound socks connection associated with the socks connection referring to the table, said table comprising for each socks connection an inbound socks connection[[.]];

building an outgoing IP Datagram with information comprised in the incoming IP Datagram; and

sending said outgoing IP Datagram on the inbound socks connection.

6. (Original) The method according to claim 2, wherein said IP Datagram comprises a Source IP Address field and a Destination IP Address field in an IP header for identifying the source device and the destination device, and a Source Port Address field and a Destination Port Address field in a Transmission Control Protocol (TCP) header for identifying the source port and the destination port on said source device and destination device.

7. (Currently amended) The method according to ~~claims 1 or 2~~ claim 1, wherein the step of determining whether the IP Datagram is originated by a socks client or a socks server comprises the step of:

determining if the value of the Destination Port field comprised in the IP Datagram is equal to the value of a destination port on a socks server or if the value of the Source Port field comprised in the IP Datagram is equal to the value of a source port on a socks server.

8. (Currently amended) The method according to ~~claims 1 or 2~~ claim 1, wherein said table is dynamic and comprises for each socks connection:

an identification of the inbound socks connection;

an identification of the associated outbound connection; and

an identification of the application level protocol used in IP Datagrams using said socks connection.

9. (Currently amended) The method according to ~~any one of the preceding claims~~ claim 1, wherein said table comprises:

for identifying each inbound socks connection:

an inbound source device address identifying the source device of the inbound socks connection[[,]];

an inbound source port address identifying the source port of the inbound socks connection[[,]];

an inbound destination device address identifying the destination device of the inbound socks connection[[,]]; and

an inbound destination port address identifying the destination port of the inbound socks connection[[,]]; and

for identifying each outbound socks connection:

an outbound source device address identifying the source device of the outbound socks connection[[,]];

an outbound source application address identifying the source port of the outbound socks connection[[,]];

an outbound destination device address identifying the destination device of the outbound socks connection[[,]]; and

an outbound destination application address identifying the destination port of the outbound socks connection[[,]].

10. (Currently amended) ~~A network device, in particular a router, comprising means adapted for carrying out the method according to any one of the preceding claims~~ A data processing system in a network device for caching Hyper Text Transfer Protocol (HTTP) data transported in an Internet Protocol (IP) Datagram sent on a socks connection established over a Transmission Control Protocol (TCP) connection between a source port on a source device and a destination port on a destination device, the data processing system comprising:

first identifying means for identifying elements of an incoming IP Datagram, comprising:

the source device;

the destination device;

the port on the source device; and

the port on the destination device;

first determining means for determining whether the incoming IP Datagram originates from a socks client or from a socks server;

in response to the incoming IP Datagram originating from a socks client:

first terminating means for terminating the TCP connection and the socks connection;

second identifying means for identifying the socks connection in a table;

third identifying means for identifying the application level protocol associated with said socks connection referring to said table, said table comprising for each socks connection an application level protocol; and

second determining means for determining whether said application level protocol is HTTP or not;

in response to said application level protocol being HTTP:

third determining means for determining whether HTTP data requested by the incoming IP Datagram resides in a local cache within the network device; and

in response to the HTTP data requested by the incoming IP Datagram residing in a local cache:

first building means for building an outgoing IP Datagram comprising requested HTTP data retrieved from the local cache; and

first sending means for sending said outgoing IP Datagram to the socks client originator of the incoming IP Datagram.

11. (Currently amended) A computer program product residing on a computer readable medium having computer readable code means for caching Hyper Text Transfer Protocol (HTTP) data transported in an Internet Protocol (IP) Datagram sent on a socks connection established over a Transmission Control Protocol (TCP) connection between a source port on a source device and a destination port on a destination device, said computer readable code means comprising the steps of:

identifying elements of an incoming IP Datagram, comprising:

the source device[[,]];

the destination device[[,]];

the port on the source device[[,]]; and

the port on the destination device[[,]];

~~of an incoming IP Datagram.~~

determining whether the incoming IP Datagram ~~is originated by~~ originates from a socks client or [[by]] from a socks server[[:]];

in response to [[If]] the incoming IP Datagram ~~is originated by~~ originating from a socks client:

terminating the TCP connection and the socks connection;

identifying the socks connection in a table;

identifying the application level protocol associated with said socks connection referring to said table, said table comprising for each socks connection an application level protocol;

determining whether said application level protocol is HTTP or not[[:]];

in response to [[If]] said application level protocol [[is]] being HTTP:

determining whether HTTP data requested by the incoming IP Datagram [[is]] resides in a local cache within the network device[[:]]; and

in response to [[If]] HTTP data requested by the incoming IP Datagram [[is]] residing in a local cache:

building an outgoing IP Datagram comprising requested HTTP data retrieved from the local cache; and

sending said outgoing IP Datagram to the socks client originator of the incoming IP Datagram.

12. (Currently amended) The computer program product according to ~~the preceding~~ claim 11, wherein:

in response to [[If]] HTTP data requested by the IP Datagram [[are]] not residing in the local cache within the network device:

identifying the outbound socks connection associated with the socks connection referring to the table, said table comprising for each socks connection an outbound socks connection[[.]];

building an outgoing IP Datagram with information comprised in the incoming IP Datagram; and

sending said outgoing IP Datagram on the outbound socks connection.

13. (New) The data processing system of claim 10, wherein:

in response to the HTTP data requested by the IP Datagram not residing in the local cache within the network device:

fourth identifying means for identifying the outbound socks connection associated with the socks connection referring to the table, said table comprising for each socks connection an outbound socks connection;

second building means for building an outgoing IP Datagram with information comprised in the incoming IP Datagram; and

second sending means for sending said outgoing IP Datagram on the outbound socks connection.

14. (New) The data processing system of claim 10, wherein said step of identifying the socks connection in a table, comprises the further steps of:

fourth determining means for determining whether the IP Datagram comprises a message for establishing a new socks connection, in particular a socks CONNECT message, or not; and

if the incoming IP Datagram comprises a message for establishing a new socks connection, in particular a socks CONNECT message:

defining means for defining an inbound socks connection between the socks client source of the incoming IP Datagram and the network device; and

updating means for updating the table with:

an identification of the socks connection;

an identification of the associated inbound socks connection; and

the application level protocol associated with the socks connection.

15. (New) The data processing system of claim 13, wherein said step of identifying the outbound socks connection associated with the socks connection referring to the table comprises the further steps of:

defining means for defining an outbound socks connection between the network device and the destination device of the incoming IP Datagram; and

associating means for associating in the table said outbound socks connection with the socks connection of the incoming IP Datagram.

16. (New) The data processing system of claim 13, wherein:

in response to the incoming IP Datagram not originating from a socks server:

second terminating means for terminating the TCP connection and the socks connection;

fifth identifying means for identifying the socks connection in the table;

sixth identifying means for identifying the application level protocol associated with said socks connection referring to said table; and

fourth determining means for determining whether said application level protocol is HTTP; and

in response to said application level protocol being HTTP:

caching means for caching HTTP data comprised in incoming IP Datagram in the local cache of the network device;

seventh identifying means for identifying the inbound socks connection associated with the socks connection referring to the table, said table comprising for each socks connection an inbound socks connection;

third building means for building an outgoing IP Datagram with information comprised in the incoming IP Datagram; and

third sending means for sending said outgoing IP Datagram on the inbound socks connection.

17. (New) The data processing system of claim 13, wherein said IP Datagram comprises a Source IP Address field and a Destination IP Address field in an IP header for identifying the source device and the destination device, and a Source Port Address field and a Destination Port Address field in a Transmission Control Protocol (TCP) header for identifying the source port and the destination port on said source device and destination device.

18. (New) The data processing system of claim 10, wherein the step of determining whether the IP Datagram is originated by a socks client or a socks server comprises the step of:

fourth determining means for determining if the value of the Destination Port field comprised in the IP Datagram is equal to the value of a destination port on a socks server or if the value of the Source Port field comprised in the IP Datagram is equal to the value of a source port on a socks server.

19. (New) The data processing system of claim 10, wherein said table is dynamic and comprises for each socks connection:

first identification means for an identification of the inbound socks connection;

second identification means for an identification of the associated outbound connection; and

third identification means for an identification of the application level protocol used in IP Datagrams using said socks connection.

20. (New) The data processing system of claim 10, wherein said table comprises:

for identifying each inbound socks connection:

fourth identifying means for an inbound source device address identifying the source device of the inbound socks connection;

fifth identifying means for an inbound source port address identifying the source port of the inbound socks connection;

sixth identifying means for an inbound destination device address identifying the destination device of the inbound socks connection; and

seventh identifying means for an inbound destination port address identifying the destination port of the inbound socks connection; and

for identifying each outbound socks connection:

eighth identifying means for an outbound source device address identifying the source device of the outbound socks connection;

ninth identifying means for an outbound source application address identifying the source port of the outbound socks connection;

tenth identifying means for an outbound destination device address identifying the destination device of the outbound socks connection; and

eleventh identifying means for an outbound destination application address identifying the destination port of the outbound socks connection.